INTRODUCTION 5300

(Revised 12/13)

Information security refers to the protection of information, information systems, equipment, software, and people from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information, regardless of its form (electronic, optical, oral, print, or other media), is critical to ensure business continuity, and protect information assets against unauthorized access, use, disclosure, disruption, modification, or destruction. Information security is also the means by which privacy of personal information held by state entities is protected.

The state's information assets, including its data processing capabilities, information technology infrastructure and data are an essential public resource. For many state entities, program operations would effectively cease in the absence of key computer systems. In some cases, public health and safety would be immediately jeopardized by the failure or disruption of a system. The non-availability of state information systems and resources can also have a detrimental impact on the state economy and the citizens who rely on state programs. Furthermore, the unauthorized acquisition, access, modification, deletion, or disclosure of information included in state entity files and databases can compromise the integrity of state programs, violate individual right to privacy, and constitute a criminal act.